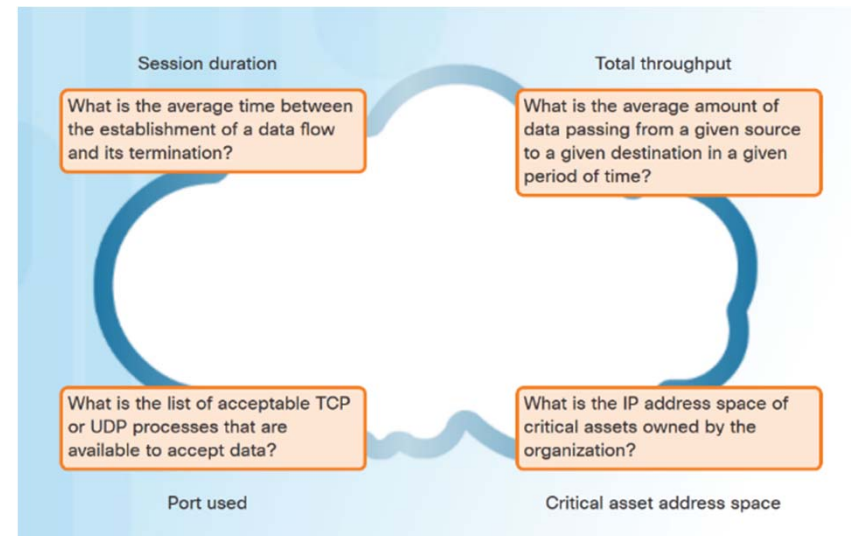


Vlerësimi i Vulnerabilitetit të Endpoint

Profilizimi i rrjetit dhe i serverit

Profilizimi i Rrjetit


- Profilizimi i rrjetit - krijoni një bazë për t'u krahasuar kundrejt kur ndodh një sulm.
- Elementet e një baze të rrjetit duhet të përfshijnë:
 - Kohëzgjatja e sesionit
 - Shpërndarja totale
 - Hapësira e adresimit të pasurisë kritike
 - Lloji tipik i trafikut



Profilizimi i rrjetit dhe i serverit

Profilizimi I Serverit

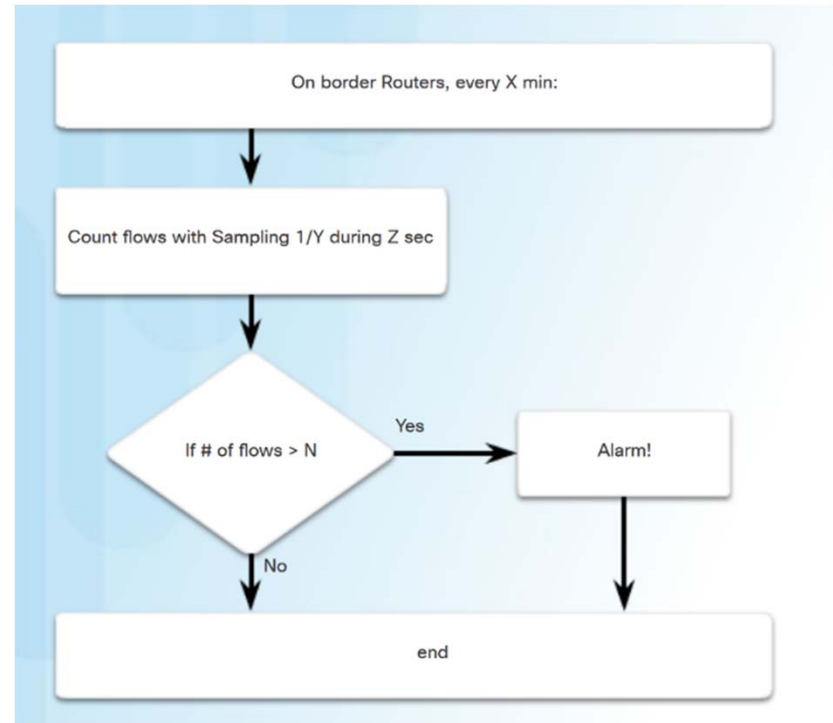
- Profilimi i serverit - përfshin portet e dëgjimit, të regjistruar në llogaritë e përdoruesve / shërbimeve, proceset e drejtimit, drejtimin e detyrave dhe aplikacionet

- 
- Listening ports
 - Logged in users/service accounts
 - Running processes
 - Running tasks
 - Applications

Profilizimi i rrjetit dhe i serverit

Zbulimi i Anomalisë së Rrjetit

- Sjellja e rrjetit përshkruhet nga një sasi e madhe e të dhënave të ndryshme siç janë tiparet e rrjedhës së paketave, tiparet e vetë paketave dhe telemetrisë nga burime të shumta.
- Teknika të analitikës së të dhënave të mëdha mund të përdoren për të analizuar këto të dhëna dhe për të zbuluar ndryshime nga linja bazë.
- Zbulimi i anomalisë mund të njohë bllokimin e rrjetit të shkaktuar nga trafiku i rrafshhtë dhe gjithashtu të identifikojë hostët e infektuar në rrjet.



Profilizimi i rrjetit dhe i serverit

Testimi i Vulnerabilitetit në Rrjet

- Testimi i vulnerabilitetit në rrjet mund të përfshijë analizën e rrezikut, vlerësimin e cenueshmërisë dhe testimin e penetrimit.

Activity	Examples	Tools
Risk Analysis	individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	internal or external consultants, risk management frameworks
Vulnerability Assessment	patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Penetration Testing	use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration.	Metasploit, CORE Impact, ethical hackers

Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS)

Përmbledhje e CVSS

- Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit (CVSS) është një vlerësim i rrezikut i dizajnuar për të përcjellë atributet e përbashkëta dhe ashpërsinë e dobësive në sistemet kompjuterike dhe softuerike.
- Rezultatet e standardizuara të cenueshmërisë
- Kornizë e hapur me metrics
- Ndhmon prioritizimin e riskut në mënyrë kuptimplote

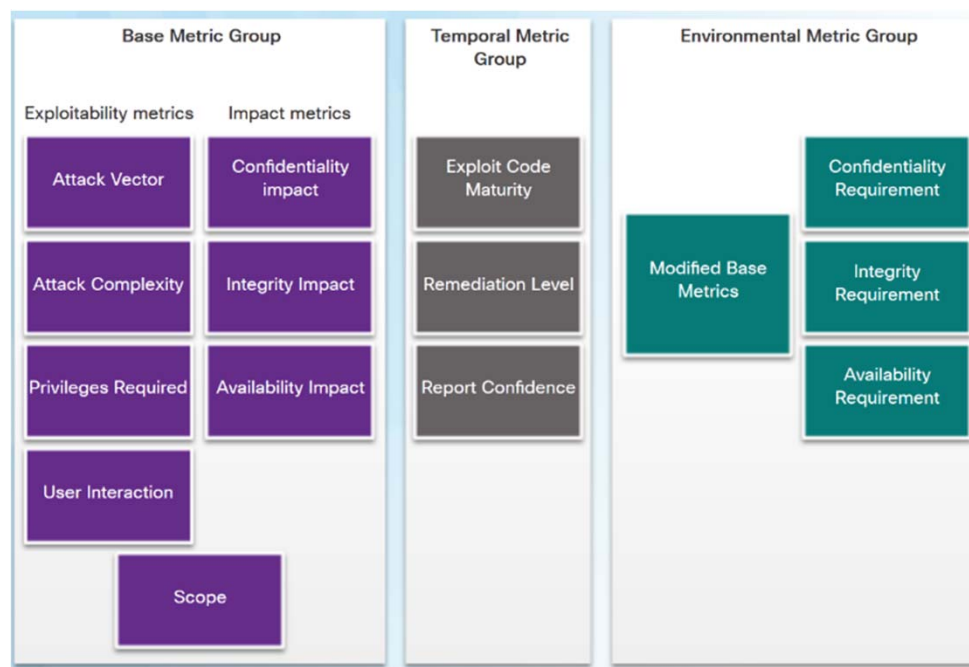
The screenshot shows the official website for the Common Vulnerability Scoring System (CVSS) v3.0. The page features the FIRST logo at the top left and social media icons at the top right. A navigation menu is visible on the left side. The main content area is titled "Common Vulnerability Scoring System v3.0: Specification Document" and includes a link to the PDF format. Below this, there is a section for "Resources & Links" which provides a table of useful references.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector string. Available at http://www.first.org/cvss/specification-document
User guide	Includes further discussion of CVSS v3.0, a scoring rubric, and a glossary. Available at http://www.first.org/cvss/user-guide
Example document	Includes examples of CVSS v3.0 scoring in practice. https://www.first.org/cvss/examples
CVSS v3.0 Calculator	This guide covers the following aspects of the CVSS Calculator: Calculator Use, Changelog, Technical Design and XML Schema Definition. Available at https://www.first.org/cvss/calculator/3.0

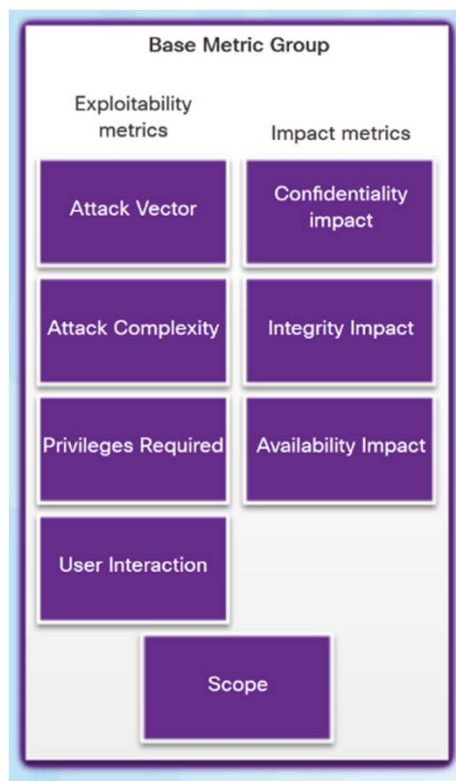
Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS)

CVSS Metric Groups

- CVSS përdor tre grupe metrikë për të vlerësuar cenueshmërinë:
 - Grupi metrikë bazë - paraqet karakteristikat e një cenueshmërie që janë konstante me kalimin e kohës dhe në kontekste të ndryshme.
 - Grupi Metrik Temporal - mat karakteristikat e një vulnerabiliteti që mund të ndryshojë me kalimin e kohës, por jo në mjediset e përdoruesit.
 - Grupi Metrik i Mjedisit - mat aspekte të një cenueshmërie që rrënjosen në një mjedis të një organizate specifike.



Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS) CVSS Base Metric Group



- Metrics Metric Metrics Bazë ekspozueshmërisë përfshijnë kriteret e mëposhtme:
 - Vektor sulm
 - Sulmo kompleksitetin
 - Privilegjet e kërkuara
 - Bashkëveprimi i përdoruesit
 - fushë
- Komponentët metrikë të ndikimit përfshijnë:
 - Ndikimi i Konfidencialitetit
 - Ndikimi i integritetit
 - Ndikimi i Disponueshmërisë

Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS)

Procesi i CVSS

- Procesi CVSS përdor një mjet të quajtur CVSS v3.0 Calculator.
- Llogaritësi është i ngjashëm me një pyetësor në të cilin bëhen zgjedhjet që përshkruajnë cenueshmërinë për secilin grup metrikë. Pastaj një rezultat është gjeneruar.
- Grupi bazë metrik përfundon së pari.
- Pastaj vlerat metrike të kohës dhe të mjedisit modifikojnë rezultatet bazë të metrikës për të dhënë një rezultat të përgjithshëm.

The screenshot displays the CVSS v3.0 Calculator interface. At the top right, the **Base Score** is shown as **3.8 (Low)**. The calculator is divided into two columns of metrics. The left column includes: **Attack Vector (AV)** with options Network (N), Adjacent (A), Local (L), and Physical (P); **Attack Complexity (AC)** with options Low (L) and High (H); **Privileges Required (PR)** with options None (N), Low (L), and High (H); and **User Interaction (UI)** with options None (N) and Required (R). The right column includes: **Scope (S)** with options Unchanged (U) and Changed (C); **Confidentiality (C)** with options None (N), Low (L), and High (H); **Integrity (I)** with options None (N), Low (L), and High (H); and **Availability (A)** with options None (N), Low (L), and High (H). At the bottom, a green box displays the **Vector String**: **CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:H**.

Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS)

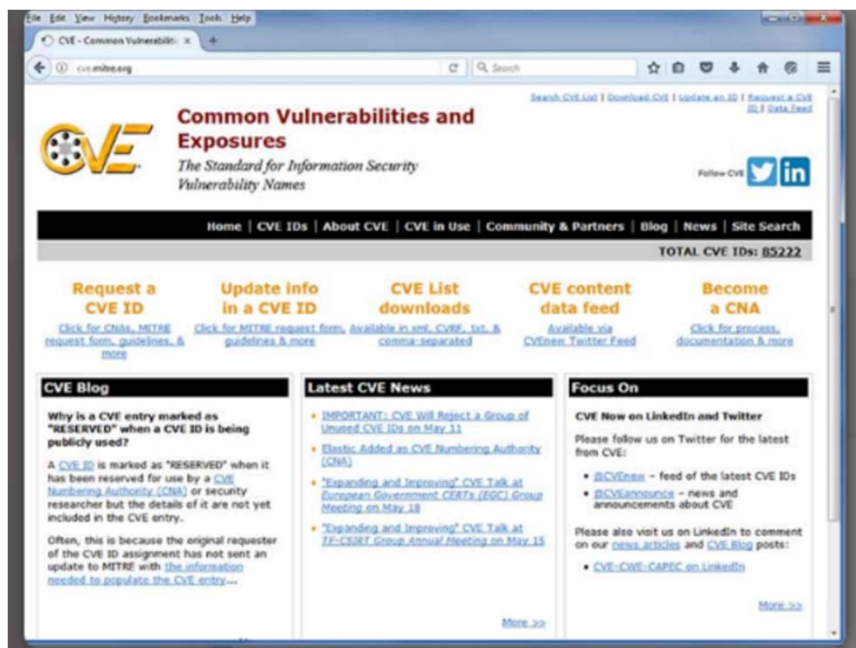
Raportet e CVSS

- Sa më i lartë vlerësimi i ashpërsisë, aq më i madh është ndikimi potencial i një shfrytëzimi dhe aq më e madhe është urgjenca në adresimin e dobësisë.
- Një dobësi që tejkalon 3.9 duhet të adresohet.

Rating	CVSS Score
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Sistemi i Përbashkët i Vlerësimit të Vulnerabilitetit Common Vulnerability Scoring System (CVSS)

Burime të tjera të Informacionit mbi Vulnerabilitetin

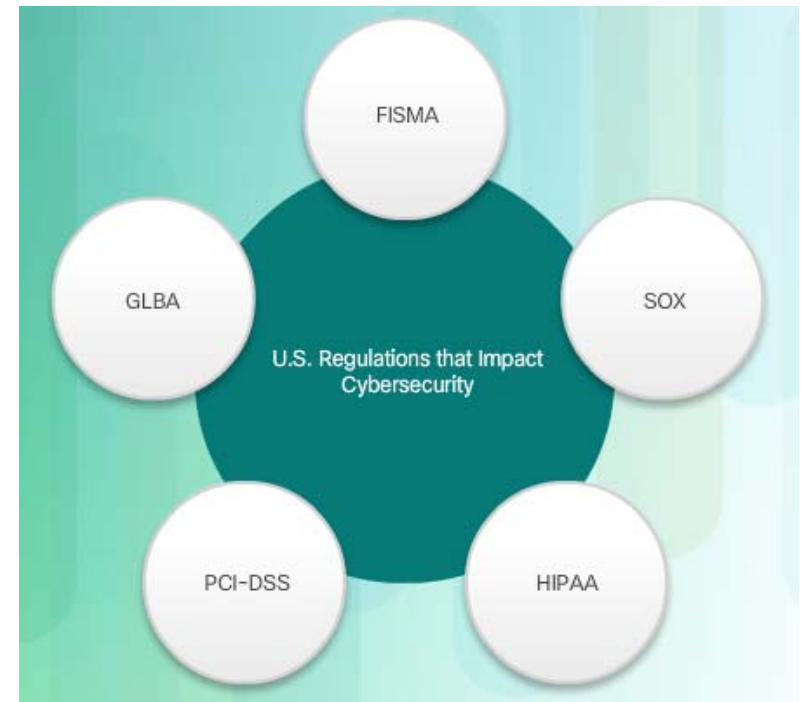


- **Cenueshmëri dhe Ekspozime të Përbashkëta (CVE)** - fjalor i emrave të zakonshëm, në formën e identifikuesve CVE, për dobësitë e njohura të sigurisë kibernetike.
- **Baza Kombëtare e Vulnerabilitetit (NVD)** - shfrytëzon identifikuesit e CVE dhe furnizon informata shitesë të tilla si rezultatet e kërcënimit të CVSS, detajet teknike, entitetet e prekura dhe burimet për hetime të mëtejshme.

Kornizat e pajtueshmërisë

Rregulloret e Pajtueshmërisë

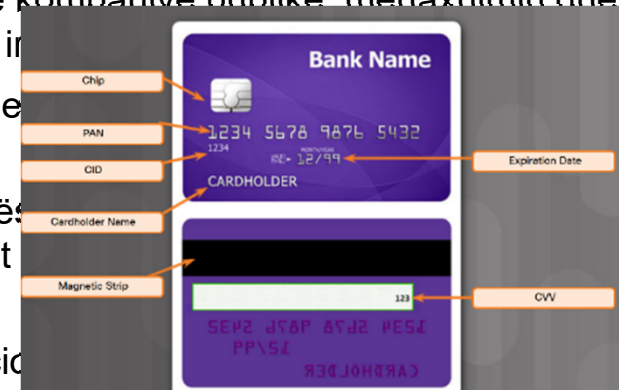
- Për të parandaluar shkeljet e sigurisë, një numër i rregullave të pajtueshmërisë së sigurisë kanë dalë.
- Rregulloret ofrojnë një kornizë për praktikën që rrisin sigurinë e informacionit, duke parashikuar gjithashtu veprimet e reagimit të incidencës dhe dënimet për mosrespektim.



Kornizat e pajtueshmërisë

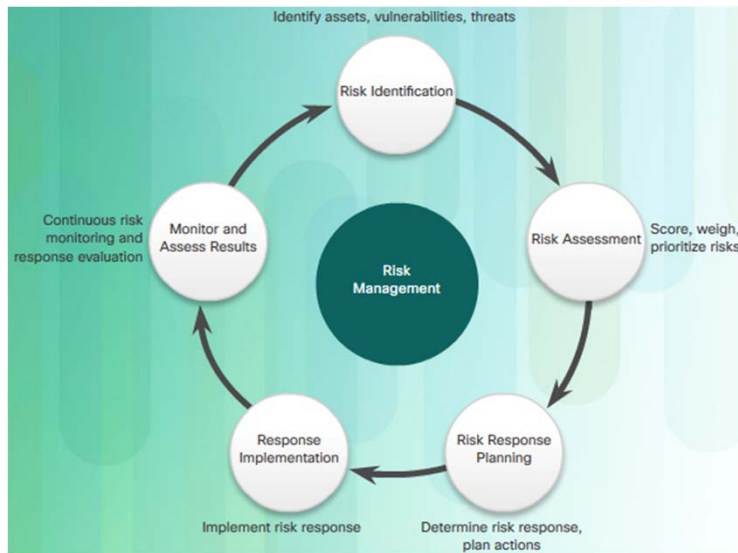
Vështrim i përgjithshëm i standardeve rregullative

- Rregullat e sigurisë në internet që ndikojnë në sigurinë kibernetike
 - FISMA (Ligji Federal për Menaxhimin e Sigurisë së Informacionit të vitit 2002) - standardet e sigurisë për sistemet qeveritare dhe kontraktorët e SHBA.
 - SOX (Sarbanes-Oxley Act of 2002) - kërkesat për bordet publike të kompanive publike, menaxhimin dhe firmat publike të kontabilitetit në lidhje me kontrollin dhe zbulimin e informacionit.
 - HIPAA (Sigurimi i Sigurimeve Shëndetësore dhe Akti i Llogaridhënieve të Kujdesit shëndetësor të pacientit).
 - PCI-DSS (Standardi i Sigurisë së të Dhënave të Industrisë së Kartës joqeveritar i krijuar nga pesë kompani të mëdha të kartës së kreditit të klientit).
 - GLBA (Gramm-Leach-Bliley Act) - kërkesat për sigurinë e informacionit të institucioneve financiare.



Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Rrezikut



- Menaxhimi i rrezikut përfshin zgjedhjen dhe specifikimin e kontrolleve të sigurisë për një organizatë.
 - Shmangia e rrezikut - Ndalo kryerjen e aktiviteteve që krijojnë rrezik.
 - Reduktimi i rrezikut - Merrni masat për të reduktuar cenueshmërinë.
 - Ndarja e rrezikut - Zhvendosni pak nga rreziku për palët e tjera.
 - Ruajtja e rrezikut - Pranoni rrezikun dhe pasojat e tij.

Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Vulnerabilitetit

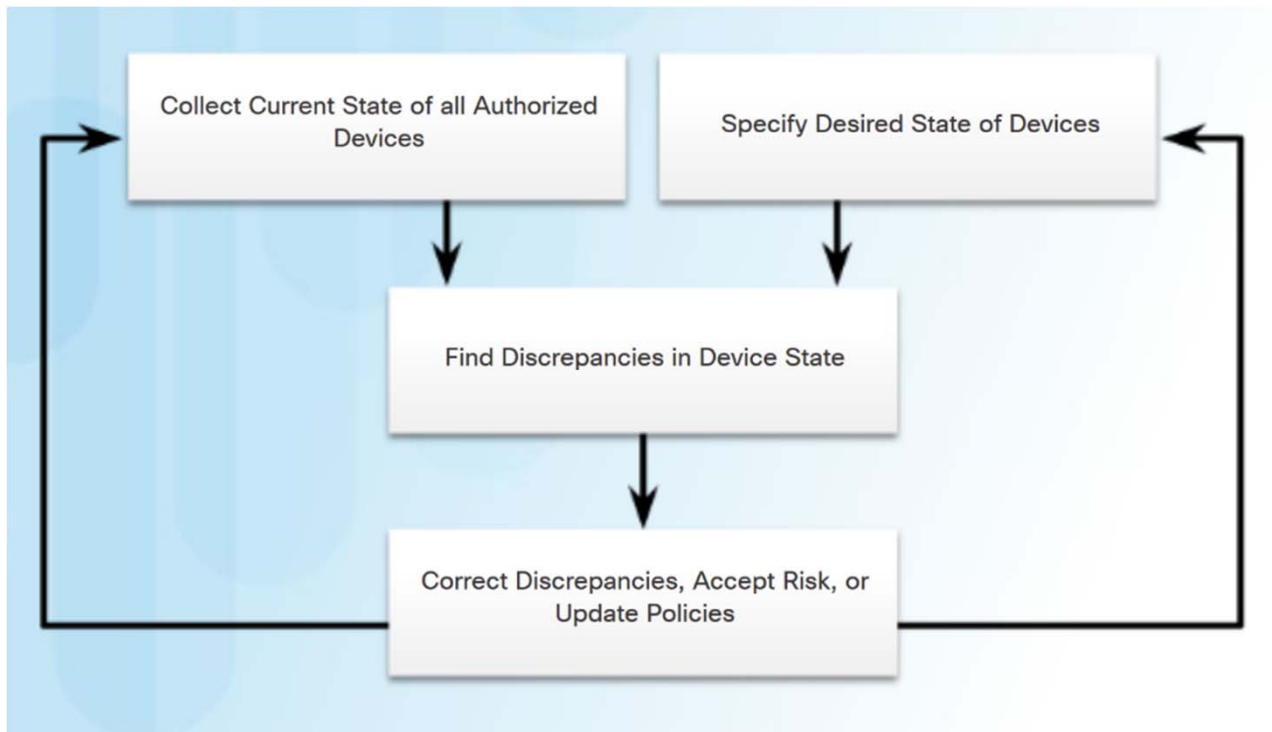
- Menaxhimi i cënueshmërisë është një praktikë e sigurisë e dizajnuar për të parandaluar në mënyrë proaktive shfrytëzimin e dobësive të TI.
- Hapat në Ciklin e Menaxhimit të Vulnerabilitetit:
 - Zbuloni - Inventoni të gjitha asetet në të gjithë rrjetin dhe identifikoni detajet e strehuesit. Zhvillimi i bazës së rrjetit. Identifikoni dobësitë e sigurisë në një orar të rregullt të automatizuar.
 - Prioritizimi i Aktiveve - Kategorizimi i aktiveve në grupe ose njësi biznesi dhe caktimi i një vlere biznesi në grupet e aseteve bazuar në kritikën e tyre ndaj veprimtarive të biznesit.
 - Vlerësoni - Përcaktoni një profil të rrezikut bazë për të eliminuar.
 - Raporti - Matni nivelin e rrezikut të biznesit që lidhet me asetet tuaja. Dokumentoni një plan sigurie, monitoroni aktivitetin e dyshimtë dhe përshkruani dobësitë e njohura.
 - Remediate - Prioritizimi sipas riskut të biznesit dhe adresimi i dobësive në rendin e rrezikut.
 - Verifiko - Verifiko se kërcënimet janë eliminuar përmes auditimeve pasuese.



Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Aseteve

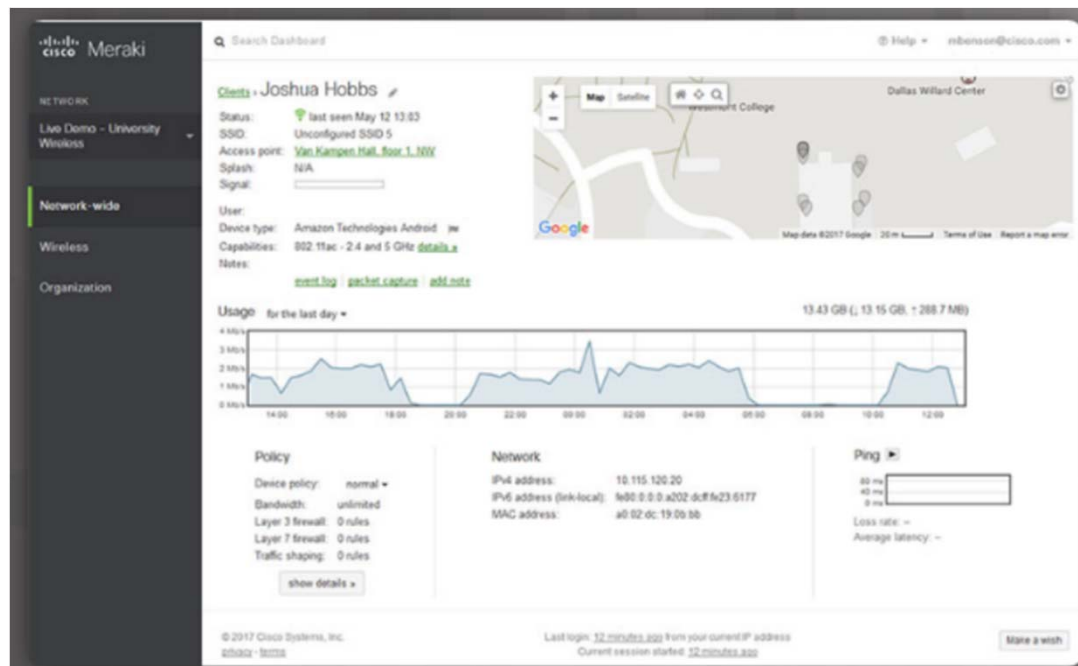
- Menaxhimi i aseteve - vendndodhja e pistave dhe konfigurimi i pajisjeve dhe softuerit



Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Pajisjeve Mobile

- Menaxhimi i pajisjeve mobile (MDM) - konfiguroni, monitoroni dhe përditësoni klientët celularë



Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Konfigurimit

- Menaxhimi i Konfigurimit - NIST Definition - përfshin një koleksion të aktiviteteve të fokusuara në krijimin dhe ruajtjen e integritetit të produkteve dhe sistemeve, përmes kontrollit të proceseve për inicializimin, ndryshimin dhe monitorimin e konfigurimeve të atyre produkteve dhe sistemeve.
- Shembuj të veglave të menaxhimit të konfiguracionit - Kukulla, e mundshme, kripëza, kuzhinier.



Menaxhimi i Sigurt i Pajisjeve

Menaxhimi i Patch Enterprise

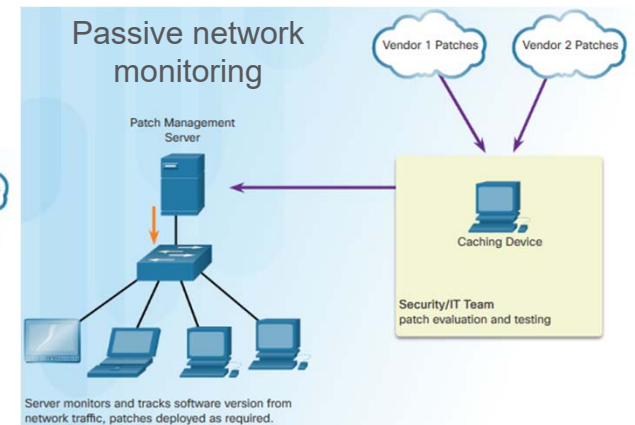
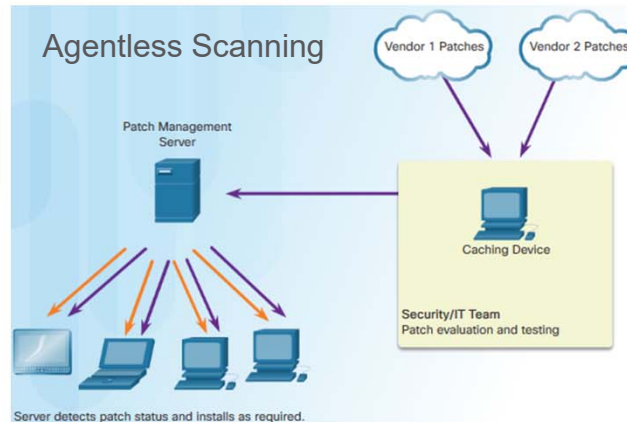
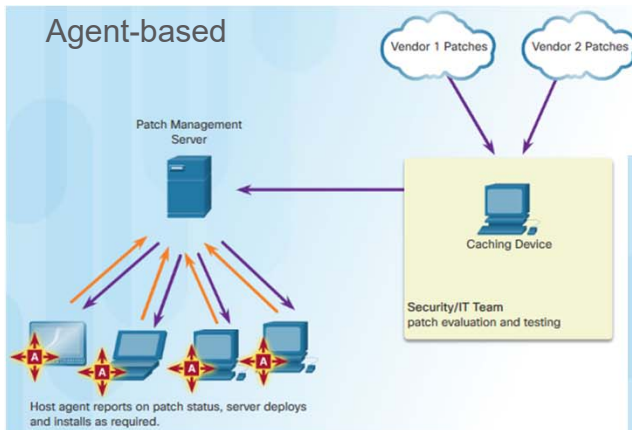
- Menaxhimi i Patch përfshin të gjitha aspektet e patching software, duke përfshirë identifikimin patches kërkuar, blerjen, shpërndarjen, instalimin dhe verifikimin se patch është instaluar në të gjitha sistemet e kërkuara.



Menaxhimi i Sigurt i Pajisjeve

Teknikat e Menaxhimit të Patch-it

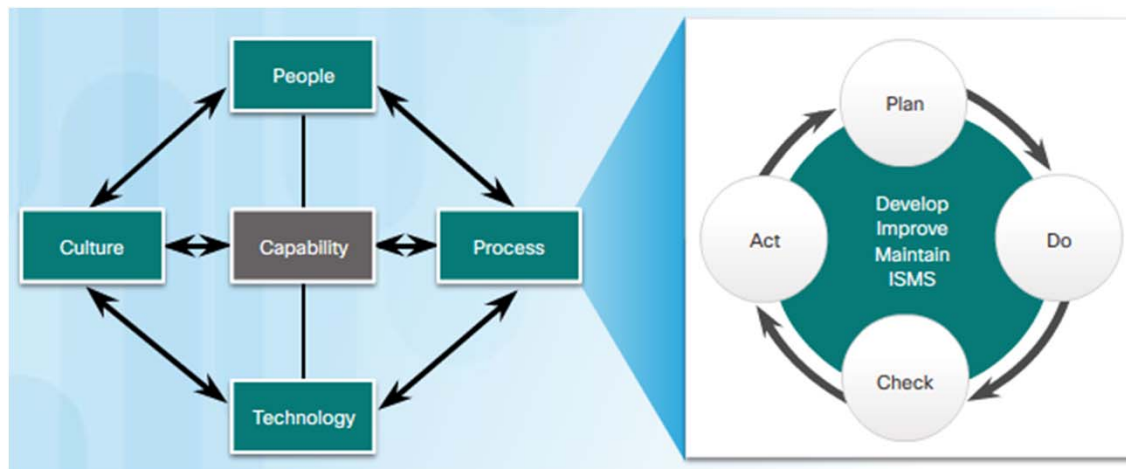
- Tre teknikat e menaxhimit të patch-it:
 - Agjenti i bazuar - software në çdo host.
 - Skanim i asgjësimit - serverët e menaxhimit të patch-it skanojnë pajisjet që kanë nevojë për patch.
 - Monitorimi i rrjetit pasiv - monitoroni trafikun e rrjetit për të identifikuar se cilat pajisje duhet të jenë patch.



Sistemet e Menaxhimit të Sigurisë së Informacionit

Sistemet e Menaxhimit të Sigurisë

- Kuadri i menaxhimit për të identifikuar, analizuar dhe adresuar rreziqet e sigurisë së informacionit
- ISMS ofrojnë modele konceptuale që udhëheqin organizatat në planifikimin, zbatimin, qeverisjen dhe vlerësimin e programeve të sigurisë së informacionit.



Sistemet e Menaxhimit të Sigurisë së Informacionit ISO-27001

- Standardi ISO / IEC 27000 i standardeve - standardet e pranuar ndërkombëtarisht që lehtësojnë biznesin e kryer midis vendeve
- Certifikimi ISO 27001 është një specifikim global për industrinë për një ISMS.



Plan

- Understand relevant business objectives
- Define scope of activities
- Access and manage support
- Assess and define risk
- Perform asset management and vulnerability assessment

Check

- Monitor implementation
- Compile reports
- Support external certification audit

Do

- Create and implement risk management plan
- Establish and enforce risk management policies and procedures
- Train personnel, allocate resources

Act

- Continually audit processes
- Continual process improvement
- Take corrective action
- Take preventive action

Sistemet e Menaxhimit të Sigurisë së Informacionit

NIST Cybersecurity Framework

- **Korniza NIST e Kibernetikës** - një sërë standardesh të dizajnuara për të integruar standardet ekzistuese, udhëzimet dhe praktikën për të ndihmuar në administrimin më të mirë dhe zvogëlimin e rrezikut të sigurisë kibernetike.

Core Function	Description
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Përmbledhje

- Hetoni dobësitë dhe sulmet në fund duke përdorur antimalar, firewall të bazuar në host dhe sistemet e zbulimit të ndërhyrjeve të bazuara në host (HIDS).
- Sipërfaqja e sulmit është e gjitha dobësitë e arritshme për një sulmues dhe mund të përfshijnë portat e hapura, aplikacionet, lidhjet pa tela dhe përdoruesit.
- Tre përbërës të sipërfaqes së sulmit: rrjeti, softueri dhe njeriu.
- Bazelimi kryhet nga profilizimi i rrjetit dhe profilizimi i serverit.
- Një profil i rrjetit mund të përmbajë kohëzgjatjen e sesionit, xhiros totale, portet e përdorura dhe hapësira kritike për adresimin e pasurive.
- Një profil i serverit zakonisht përmban porte dëgjimi, të regjistruar në llogaritë e përdoruesve / shërbimit, proceset e drejtimit, drejtimin e detyrave dhe aplikacionet.
- Testimi i cënueshmërisë së rrjetit kryhet duke përdorur analizën e rrezikut, vlerësimin e cënueshmërisë dhe testimin e penetrimit.
- CVSS është një vlerësim i rrezikut vendor-neutral që përmban tre grupe kryesore metrike (baza, afati kohor dhe mjedisi). Secili grup ka metrika specifike që mund të maten.

Përmbledhje

- Rregulloret e pajtueshmërisë përfshijnë FISMA, SOX, HIPAA, PCI-DSS dhe GLBA.
- Menaxhimi i rrezikut përdoret për të identifikuar pasuritë, dobësitë dhe kërcënimet.
- 4 metodat e reduktimit të rrezikut përfshijnë shmangien e rrezikut, uljen e rrezikut, ndarjen e rrezikut dhe mbajtjen e rrezikut
- Menaxhimi i cënueshmërisë parandalon në mënyrë aktive shfrytëzimin e dobësive të TI. 6 hapat e ciklit jetësor të menaxhimit të cënueshmërisë përfshijnë zbulimin, prioritizimin e pasurisë, vlerësimin, raportimin, riparimin dhe verifikimin.
- Menaxhime të tjera të pajisjeve që duhet të konsiderohen përfshijnë menaxhimin e aseteve, menaxhimin e pajisjeve mobile, menaxhimin e konfigurimit dhe menaxhimin e patch-it.
- Një ISMS përbëhet nga një kuadër menaxhimi i përdorur për të identifikuar, analizuar dhe adresuar rreziqet e sigurisë së informacionit. Shembujt përfshijnë familjen ISO / IEC 27000 të standardeve dhe Core dhe Funksionet e Kornizës së Cybersecurity NIST.